(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－109856

(43)公開日　平成11年(1999)４月23日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６３０	Ｇ０９Ｃ	1/00	６３０Ａ
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ａ
	12/14	３２０		12/14	３２０Ｂ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ａ

審査請求　未請求　請求項の数14　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－267515

(22)出願日　平成９年(1997)９月30日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(71)出願人　390020248
日本テキサス・インスツルメンツ株式会社
東京都港区北青山３丁目６番12号　青山富士ビル

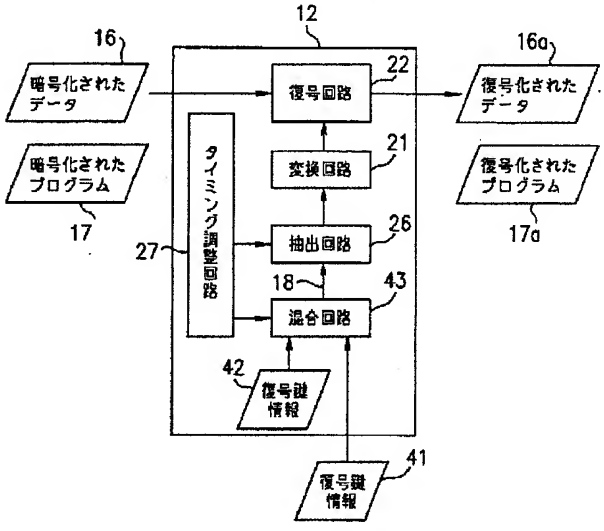
(72)発明者　金光　朋彦
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　山本　秀策

最終頁に続く

(54)【発明の名称】　復号装置

(57)【要約】
【課題】　復号鍵情報を不正に取得した第三者が暗号化されたプログラムまたは暗号化されたデータを容易に復号化することを防止する。
【解決手段】　復号装置１２は、復号鍵情報４１と復号鍵情報４２とに基づいて、復号鍵１８ａを生成する復号鍵生成回路（４３、２６、２１）と、復号鍵１８ａを用いて暗号化された情報を復号化する復号回路２２とを備えている。復号鍵情報４１は、復号装置１２の外部から入力される。復号鍵情報４２は、復号装置１２の内部に格納されている。



1

【特許請求の範囲】

【請求項１】　第１復号鍵情報と第２復号鍵情報とに基づいて、復号鍵を生成する復号鍵生成回路と、
前記復号鍵を用いて、暗号化された情報を復号化する復号回路とを備えた復号装置であって、
前記第１復号鍵情報は、前記復号装置の外部から入力され、
前記第２復号鍵情報は、前記復号装置の内部に格納されている、復号装置。

【請求項２】　前記暗号化された情報は、暗号化されたプログラムである、請求項１に記載の復号装置。

【請求項３】　前記暗号化された情報は、暗号化されたデータである、請求項１に記載の復号装置。

【請求項４】　前記復号鍵生成回路は、
前記第１復号鍵情報と前記第２復号鍵情報とを混合することにより、復号鍵情報を生成する混合回路と、
前記復号鍵情報を前記復号鍵に変換する変換回路とを含む、請求項１に記載の復号装置。

【請求項５】　前記第１復号鍵情報は、前記復号鍵に関連する情報と前記復号鍵に関連しないダミーデータとを含む、請求項１に記載の復号装置。

【請求項６】　前記第２復号鍵情報は、複数の復号鍵を含んでおり、
前記復号鍵生成回路は、前記複数の復号鍵のうち１つを選択する選択回路を含む、請求項１に記載の復号装置。

【請求項７】　前記第２復号鍵情報は、複数の復号鍵情報を含んでおり、
前記復号鍵生成回路は、
前記複数の復号鍵情報のうち１つを選択する選択回路と、
前記選択回路によって選択された復号鍵情報を復号鍵に変換する変換回路とを含む、請求項１に記載の復号装置。

【請求項８】　復号鍵情報を復号鍵に変換する第１変換回路と、
前記復号鍵を用いて、暗号化された情報を復号化する復号回路とを備え、
前記復号鍵情報は、前記復号鍵に関連する情報と前記復号鍵に関連しないダミーデータとを含む、復号装置。

【請求項９】　前記暗号化された情報は、暗号化されたプログラムである、請求項８に記載の復号装置。

【請求項１０】　前記暗号化された情報は、暗号化されたデータである、請求項８に記載の復号装置。

【請求項１１】　前記復号鍵に関連する情報は、前記復号鍵を含んでおり、前記第１変換回路は、前記復号鍵情報から前記復号鍵を抽出する抽出回路を含む、請求項８に記載の復号装置。

【請求項１２】　前記第１変換回路は、
前記復号鍵情報から前記復号鍵に関連する情報を抽出する抽出回路と、

2

前記復号鍵に関連する情報を前記復号鍵に変換する第２変換回路とを含む、請求項８に記載の復号装置。

【請求項１３】　前記暗号化された情報は、前記復号装置に関連して設けられたメモリに格納されている、請求項１または請求項８のいずれかに記載の復号装置。

【請求項１４】　前記復号装置は、入力されたアドレスを一定の規則に従って変換し、変換されたアドレスを前記メモリに出力するアドレスシャッフル回路をさらに備えており、前記変換されたアドレスに従って前記メモリから読み出された前記暗号化された情報が前記復号回路に供給される、請求項１３に記載の復号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、復号鍵を用いて暗号化されたプログラムまたは暗号化されたデータを復号化する復号装置に関する。

【０００２】

【従来の技術】従来、データを暗号化して保存し、そのデータを暗号化するのに使用した鍵をマスタ鍵を用いて暗号化して保存する手法が提案されている（例えば、辻井重男、笠原正雄著「暗号と情報セキュリティ」、第２０８頁～第２１２頁、昭晃堂、１９９０年）。

【０００３】上記文献は、そのように暗号化されたデータを復号化する復号装置を開示している。復号装置には、暗号化されたデータとマスタ鍵K_Mとが入力される。復号装置は、暗号化されたデータのヘッダ部分にある鍵K_Eを抽出し、鍵K_Eをレジスタに格納する。復号装置は、鍵K_Eとマスタ鍵K_Mとに基づいてワーク鍵K_Wを生成し、ワーク鍵K_Wを用いて暗号化されたデータを復号化する。

【０００４】このような復号装置をプロセッサの内部に持つこととすると、外部から参照できるのは、暗号化されたデータと、暗号化された鍵K_Mと、マスタ鍵K_Mとである。従って、マスタ鍵K_Mを機密に管理することにより、暗号化されたデータを保護することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、上述した従来技術によれば、マスタ鍵K_Mとワーク鍵K_Wの間に相関があるので、マスタ鍵K_Mがわかってしまうと、暗号化アルゴリズムが既知の場合には暗号化されたデータが比較的容易に復号化されてしまうという問題点があった。

【０００６】このため、従来では、マスタ鍵K_Mの機密レベルを高く設定する必要があった。このことは、マスタ鍵K_Mを復号装置に転送するために必要とされる回路の規模を増大させるという問題点があった。

【０００７】本発明は、上記問題点に鑑みてなされたものであり、復号鍵情報を不正に取得した第三者が暗号化されたプログラムまたは暗号化されたデータを容易に復号化することを防止する復号装置を提供することを目的

とする。また、復号鍵情報を復号装置に転送するために必要とされる回路の規模を削減することのできる復号装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明の復号装置は、第１復号鍵情報と第２復号鍵情報とに基づいて、復号鍵を生成する復号鍵生成回路と、前記復号鍵を用いて、暗号化された情報を復号化する復号回路とを備え、前記第１復号鍵情報は、前記復号装置の外部から入力され、前記第２復号鍵情報は、前記復号装置の内部に格納されている。これにより、上記目的が達成される。

【０００９】前記暗号化された情報は、暗号化されたプログラムであってもよい。

【００１０】前記暗号化された情報は、暗号化されたデータであってもよい。

【００１１】前記復号鍵生成回路は、前記第１復号鍵情報と前記第２復号鍵情報とを混合することにより、復号鍵情報を生成する混合回路と、前記復号鍵情報を前記復号鍵に変換する変換回路とを含んでいてもよい。

【００１２】前記第１復号鍵情報は、前記復号鍵に関連する情報と前記復号鍵に関連しないダミーデータとを含んでいてもよい。

【００１３】前記第２復号鍵情報は、複数の復号鍵を含んでおり、前記復号鍵生成回路は、前記複数の復号鍵のうち１つを選択する選択回路を含んでいてもよい。

【００１４】前記第２復号鍵情報は、複数の復号鍵情報を含んでおり、前記復号鍵生成回路は、前記複数の復号鍵情報のうち１つを選択する選択回路と、前記選択回路によって選択された復号鍵情報を復号鍵に変換する変換回路とを含んでいてもよい。

【００１５】本発明の他の復号装置は、復号鍵情報を復号鍵に変換する第１変換回路と、前記復号鍵を用いて、暗号化された情報を復号化する復号回路とを備え、前記復号鍵情報は、前記復号鍵に関連する情報と前記復号鍵に関連しないダミーデータとを含む。これにより、上記目的が達成される。

【００１６】前記暗号化された情報は、暗号化されたプログラムであってもよい。

【００１７】前記暗号化された情報は、暗号化されたデータであってもよい。

【００１８】前記復号鍵に関連する情報は、前記復号鍵を含んでおり、前記第１変換回路は、前記復号鍵情報から前記復号鍵を抽出する抽出回路を含んでいてもよい。

【００１９】前記第１変換回路は、前記復号鍵情報から前記復号鍵に関連する情報を抽出する抽出回路と、前記復号鍵に関連する情報を前記復号鍵に変換する第２変換回路とを含んでいてもよい。

【００２０】前記暗号化された情報は、前記復号装置に関連して設けられたメモリに格納されていてもよい。

【００２１】前記復号装置は、入力されたアドレスを一定の規則に従って変換し、変換されたアドレスを前記メモリに出力するアドレスシャッフル回路をさらに備えており、前記変換されたアドレスに従って前記メモリから読み出された前記暗号化された情報が前記復号回路に供給されてもよい。

【００２２】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を説明する。

【００２３】（実施の形態１）図１は、本発明の復号装置１２を含むプロセッサチップ１１の構成を示す。プロセッサチップ１１は、復号装置１２とインタフェース１３とプロセッサコア１５とを含む。

【００２４】復号鍵情報１８は、インタフェース１３およびバス１４を介して、復号装置１２に入力される。インタフェース１３は、復号鍵情報の入力に特化されたものである必要はない。例えば、インタフェース１３は、プロセッサチップ１１内に設けられている各種のレジスタ（図示せず）に設定する値１９などを入力するためにも使用され得る。

【００２５】暗号化されたデータ１６は、復号装置１２に入力される。復号装置１２は、復号鍵情報１８を用いて、暗号化されたデータ１６を復号化する。復号化されたデータはプロセッサコア１５に供給される。復号鍵情報１８および復号処理の詳細は、図２（ａ）～（ｃ）を参照して後述される。

【００２６】暗号化されたプログラム１７は、復号装置１２に入力される。復号装置１２は、復号鍵情報１８を用いて、暗号化されたプログラム１７を復号化する。復号化されたプログラムはプロセッサコア１５に直接的に供給される。あるいは、復号化されたプログラムはプログラムローダ（図示せず）に供給されてもよい。復号化されたプログラムが実行されると、プロセッサチップ１１内に設けられているプログラムメモリ（図示せず）や各種のレジスタ（図示せず）に値が設定される。

【００２７】なお、暗号化されたデータ１６と暗号化されたプログラム１７とがプロセッサチップ１１に同時に入力される形態も考えられる。この場合、例えば、復号装置１２を２個並列に配置し、暗号化されたデータ１６を一方の復号装置に入力し、暗号化されたプログラム１７を他方の復号装置に入力するようにすればよい。

【００２８】図２（ａ）は、復号装置１２の構成を示す。復号装置１２は、復号鍵情報１８から復号鍵に関連する情報を抽出する抽出回路２６と、抽出回路２６によって抽出された復号鍵に関連する情報を復号鍵に変換する変換回路２１と、復号鍵を用いて暗号化されたデータ１６または暗号化されたプログラム１７を復号化する復号回路２２とを含んでいる。

【００２９】復号鍵情報１８は、復号鍵に関連する情報と、復号鍵に関連しないダミーデータとを含んでいる。復号鍵に関連する情報は、復号鍵自身であってもよい

し、復号鍵と相関を持った値であってもよい。

【００３０】図２（ｂ）は、復号鍵情報１８の構成例を示す。復号鍵情報１８は、復号鍵１８ａと、復号鍵１８ａに関連しないダミーデータ１８ｂとを含む。復号鍵情報１８における復号鍵１８ａの位置は予め決められている。復号鍵１８ａの位置は、例えば、復号鍵情報１８の先頭から５０バイト目であり得る。復号鍵情報１８において、復号鍵１８ａ以外の部分をダミーデータ１８ｂで埋めることにより、仮に第三者が復号鍵情報１８を得た場合でも復号鍵情報１８の中から復号鍵１８ａを特定することは困難である。

【００３１】図２（ｃ）は、復号鍵情報１８の他の構成例を示す。復号鍵情報１８は、復号鍵１８ａと相関を持った値１８ｃ（以下、相関値１８ｃという）と、復号鍵１８ａに関連しないダミーデータ１８ｂとを含む。復号鍵情報１８における相関値１８ｃの位置は予め決められている。相関値１８ｃの位置は、例えば、復号鍵情報１８の先頭から５０バイト目であり得る。復号鍵情報１８において、相関値１８ｃ以外の部分をダミーデータ１８ｂで埋めることにより、仮に第三者が復号鍵情報１８を得た場合でも復号鍵情報１８の中から相関値１８ｃを特定することは困難である。

【００３２】このように、復号鍵１８ａに関連しないダミーデータを使用することにより、復号鍵情報１８の秘匿性を高めることができる。これにより、復号鍵情報１８の機密レベルを下げることができる。その結果、復号鍵情報１８を復号装置１２に転送するために必要とされる回路の規模を削減することができる。

【００３３】図２（ａ）を再び参照して、復号鍵情報１８が入力された場合の復号装置１２の動作を説明する。

【００３４】図２（ｂ）に示す構成を有する復号鍵情報１８が入力された場合には、抽出回路２６は、復号鍵情報１８から復号鍵１８ａを抽出する。復号鍵１８ａを抽出するタイミングは、タイミング調整回路２７から出力されるイネーブル信号によって制御される。抽出回路２６によって抽出された復号鍵１８ａは、変換回路２１をスルーして復号回路２２に供給される。従って、復号鍵情報１８が図２（ｂ）に示す構成を有する場合には、変換回路２１は省略され得る。復号回路２２は、復号鍵１８ａを用いて暗号化されたデータ１６または暗号化されたプログラム１７を復号化する。その結果、復号化されたデータ１６ａまたは復号化されたプログラム１７ａが復号回路２２から出力される。

【００３５】図２（ｃ）に示す構成を有する復号鍵情報１８が入力された場合には、抽出回路２６は、復号鍵情報１８から相関値１８ｃを抽出する。相関値１８ｃを抽出するタイミングは、タイミング調整回路２７から出力されるイネーブル信号によって制御される。抽出回路２６によって抽出された相関値１８ｃは、変換回路２１に供給される。変換回路２１は、相関値１８ｃを復号鍵１８ａに変換する。ここで、復号鍵１８ａを正しく得るためには、相関値１８ｃが所定の規則に従って復号鍵１８ａを導くことができる値であり、かつ、その所定の規則が変換回路２１に予め反映されていることが必要とされる。例えば、相関値１８ｃが復号鍵１８ａを可逆変換した値である場合には、相関値１８ｃから復号鍵１８ａを導く式が変換回路２１に設定されている必要がある。復号回路２２は、復号鍵１８ａを用いて暗号化されたデータ１６または暗号化されたプログラム１７を復号化する。その結果、復号化されたデータ１６ａまたは復号化されたプログラム１７ａが復号回路２２から出力される。

【００３６】図３は、抽出回路２６に入力される復号鍵情報１８のタイミングとタイミング調整回路２７から出力されるイネーブル信号のタイミングとの関係を示す。図３に示すように、イネーブル信号がＨｉｇｈである期間中、復号鍵情報１８から復号鍵１８ａ（または相関値１８ｃ）が切り出され、その切り出されたデータが変換回路２１に供給される。

【００３７】（実施の形態２）図４は、復号装置１２の他の構成を示す。復号装置１２とその周辺回路との関係は、図１に示すとおりである。

【００３８】図４に示される復号装置１２は、復号鍵情報４１と復号鍵情報４２とを混合することにより、復号鍵情報１８を生成する混合回路４３と、復号鍵情報１８から復号鍵に関連する情報を抽出する抽出回路２６と、抽出回路２６によって抽出された復号鍵に関連する情報を復号鍵に変換する変換回路２１と、復号鍵を用いて暗号化されたデータ１６または暗号化されたプログラム１７を復号化する復号回路２２とを含んでいる。

【００３９】復号鍵情報４１は、復号装置１２の外部から入力される。一方、復号鍵情報４２は、復号装置１２の内部に格納されている。復号鍵情報４２を復号装置１２の内部に格納するために、例えば、復号鍵情報４２をプロセッサチップ１１に設けられているＲＯＭ（図示せず）に格納するようにしてもよい。あるいは、復号鍵情報４２をハードワイヤードロジックを用いて復号装置１２の内部に記憶するようにしてもよい。

【００４０】このように、復号鍵を生成するために使用される情報の一部（すなわち、復号鍵情報４２）が復号装置１２の内部に格納されているため、第三者が復号鍵情報４２を不正に取得することは困難である。第三者が復号鍵情報４２を不正に取得するためには、第三者は電子顕微鏡などを用いて復号装置１２の内部の回路を読みとらなければならないからである。近年、ＬＳＩのプロセスルールは微細化し、回路規模も増大する傾向にある。従って、復号装置１２の内部の回路を読みとる作業はきわめて困難である。復号鍵情報４２をＲＯＭに格納する方法と、復号鍵情報４２をハードワイヤードロジックを用いて復号装置１２の内部に記憶する方法とを比較

すると、前者は後者に比べて回路規模が小さくすむという利点を有するが、第三者が電子顕微鏡などを用いて回路を読みとることが容易であるという欠点を有する。従って、復号鍵情報４２の秘匿性を高めるためには後者の方法を採用することが好ましい。

【００４１】また、復号鍵を生成するために使用される情報の一部（すなわち、復号鍵情報４２）が復号装置１２の内部に格納されているため、第三者が復号鍵情報４１を得た場合でも復号鍵を知ることは困難である。復号鍵は、復号鍵情報４１と復号鍵情報４２とに基づいて生成されるからである。これにより、復号装置１２の外部から入力される復号鍵情報４１の機密レベルを下げることができる。その結果、復号鍵情報４１を復号装置１２に転送するために必要とされる回路の規模を削減することができる。

【００４２】次に、図４を参照して、復号鍵情報４１が入力された場合の復号装置１２の動作を説明する。

【００４３】混合回路４３は、復号鍵情報４１と復号鍵情報４２とを混合することにより、復号鍵情報１８を生成する。復号鍵情報１８は、例えば、図２（ｂ）に示す構成を有する。あるいは、復号鍵情報１８は、図２（ｃ）に示す構成を有していてもよい。抽出回路２６、変換回路２１、復号回路２２およびタイミング制御回路２７の動作は、図２（ａ）を参照して説明したそれらの動作と同一である。

【００４４】復号鍵情報１８を正しく得るためには、復号鍵情報１８が所定の規則に従って復号鍵情報４１と復号鍵情報４２とに分割されており、かつ、その所定の規則が混合回路４３に予め反映されていることが必要とされる。例えば、復号鍵情報１８が１００バイトのデータである場合、復号鍵情報１８の前半５０バイトのデータを復号鍵情報４１として復号装置１２の外部から入力し、復号鍵情報１８の後半５０バイトのデータを復号鍵情報４２として復号装置１２の内部に格納するようにしてもよい。この場合には、混合回路４３は、復号鍵情報４１（５０バイト）の末尾に復号鍵情報４２（５０バイト）を結合することにより、復号鍵情報１８（１００バイト）を生成する。なお、復号鍵情報１８を復号鍵情報４１と復号鍵情報４２とに分割する方法としては、任意の方法を採用することができる。

【００４５】図５は、復号装置１２の他の構成を示す。復号装置１２とその周辺回路との関係は、図１に示すとおりである。

【００４６】図５に示される復号装置１２は、復号鍵選択情報５５に応じて復号鍵α、復号鍵β、復号鍵γのうちの１つを選択する選択回路５４と、選択回路５４によって選択された復号鍵を用いて暗号化されたデータ１６または暗号化されたプログラム１７を復号化する復号回路２２とを含んでいる。

【００４７】復号鍵選択情報５５は、復号装置１２の外部から入力される。一方、復号鍵α、復号鍵β、復号鍵γは、いずれも、復号装置１２の内部に格納されている。復号鍵α、復号鍵β、復号鍵γを復号装置１２の内部に格納する方法としては、上述した復号鍵情報４２を復号装置１２の内部に格納する方法と同様の方法が採用され得る。例えば、復号鍵α、復号鍵β、復号鍵γをプロセッサチップ１１に設けられているＲＯＭ（図示せず）に格納する場合には、復号鍵αはＲＯＭの格納位置５１に格納され、復号鍵βはＲＯＭの格納位置５２に格納され、復号鍵γはＲＯＭの格納位置５３に格納され得る。

【００４８】このように、復号鍵を生成するために使用される情報の一部（すなわち、復号鍵α、復号鍵β、復号鍵γ）が復号装置１２の内部に格納されているため、第三者が復号鍵選択情報５５を得た場合でも復号鍵を知ることは困難である。復号鍵選択情報５５の値は、復号鍵α、復号鍵β、復号鍵γの値とは無関係な値とすることができるからである。これにより、復号装置１２の外部から入力される復号鍵選択情報５５の機密レベルを下げることができる。その結果、復号鍵選択情報５５を復号装置１２に転送するために必要とされる回路の規模を削減することができる。

【００４９】次に、図５を参照して、復号鍵選択情報５５が入力された場合の復号装置１２の動作を説明する。

【００５０】選択回路５４は、復号鍵選択情報５５に応じて、復号鍵α、復号鍵β、復号鍵γのうちの１つを選択する。例えば、選択回路５４は、復号鍵選択情報５５が値０を有する場合に復号鍵αを選択し、復号鍵選択情報５５が値１を有する場合に復号鍵βを選択し、復号鍵選択情報５５が値２を有する場合に復号鍵γを選択する。復号鍵選択情報５５の値と選択されるべき復号鍵との対応関係は任意に設定され得る。復号回路２２は、選択回路５４によって選択された復号鍵を用いて暗号化されたデータ１６または暗号化されたプログラム１７を復号化する。その結果、復号化されたデータ１６ａまたは復号化されたプログラム１７ａが復号回路２２から出力される。

【００５１】なお、復号装置１２の内部に格納される復号鍵の数は３に限定されない。復号装置１２の内部に格納される復号鍵の数は任意の正の整数であり得る。

【００５２】なお、復号鍵の代わりに、復号鍵とダミーデータとを含む復号鍵情報を復号装置１２の内部に格納するようにしてもよい。この場合には、復号鍵情報から復号鍵を抽出する抽出回路を復号回路２２の前段に設ければよい。また、復号鍵選択情報５５がダミーデータを含んでいてもよい。この場合には、復号鍵選択情報５５から復号鍵に対応する値を抽出する抽出回路を選択回路５４の前段に設ければよい。

【００５３】図６は、復号装置１２の他の構成を示す。復号装置１２とその周辺回路との関係は、図１に示すと

おりである。

【００５４】図６に示される復号装置１２は、復号鍵選択情報５５に応じて復号鍵と相関を持つ値α（以下、相関値αという）、復号鍵と相関を持つ値β（以下、相関値βという）、復号鍵と相関を持つ値γ（以下、相関値γという）のうちの１つを選択する選択回路５４と、選択回路５４によって選択された相関値を復号鍵に変換する変換回路２１と、復号鍵を用いて暗号化されたデータ１６または暗号化されたプログラム１７を復号化する復号回路２２とを含んでいる。

【００５５】復号鍵選択情報５５は、復号装置１２の外部から入力される。一方、相関値α、相関値β、相関値γは、いずれも、復号装置１２の内部に格納されている。相関値α、相関値β、相関値γを復号装置１２の内部に格納する方法としては、上述した復号鍵情報４２を復号装置１２の内部に格納する方法と同様の方法が採用され得る。例えば、相関値α、相関値β、相関値γをプロセッサチップ１１に設けられているＲＯＭ（図示せず）に格納する場合には、相関値αはＲＯＭの格納位置５６に格納され、相関値βはＲＯＭの格納位置５７に格納され、相関値γはＲＯＭの格納位置５８に格納され得る。

【００５６】図６に示す例では、図５に示される復号鍵α、復号鍵β、復号鍵γの代わりに、相関値α、相関値β、相関値γが復号装置１２の内部に格納されているため、第三者が復号鍵選択情報５５を得た場合でも復号鍵を知ることは一層困難である。

【００５７】次に、図６を参照して、復号鍵選択情報５５が入力された場合の復号装置１２の動作を説明する。

【００５８】選択回路５４は、復号鍵選択情報５５に応じて、相関値α、相関値β、相関値γのうちの１つを選択する。例えば、選択回路５４は、復号鍵選択情報５５が値０を有する場合に相関値αを選択し、復号鍵選択情報５５が値１を有する場合に相関値βを選択し、復号鍵選択情報５５が値２を有する場合に相関値γを選択する。復号鍵選択情報５５の値と選択されるべき相関値との対応関係は任意に設定され得る。変換回路２１は、選択回路５４によって選択された相関値を復号鍵に変換する。復号回路２２は、復号鍵を用いて暗号化されたデータ１６または暗号化されたプログラム１７を復号化する。その結果、復号化されたデータ１６ａまたは復号化されたプログラム１７ａが復号回路２２から出力される。

【００５９】なお、復号装置１２の内部に格納される相関値の数は３に限定されない。復号装置１２の内部に格納される相関値の数は任意の正の整数であり得る。

【００６０】なお、相関値の代わりに、相関値とダミーデータとを含む復号鍵情報を復号装置１２の内部に格納するようにしてもよい。この場合には、復号鍵情報から相関値を抽出する抽出回路を変換回路２１の前段に設ければよい。また、復号鍵選択情報５５がダミーデータを含んでいてもよい。この場合には、復号鍵選択情報５５から相関値に対応する値を抽出する抽出回路を選択回路５４の前段に設ければよい。

【００６１】なお、図４～図６に示される実施の形態を任意に組み合わせた実施の形態も、本発明の範囲に含まれる。

【００６２】（実施の形態３）図７は、復号装置１２の他の構成を示す。図７に示される復号装置１２は、プログラム保存用メモリ６１にアドレスを提供するアドレスシャッフル回路６２と、暗号化されたプログラム１７のうちアドレスによって指定される命令を復号化する復号回路２２とを含んでいる。

【００６３】プログラム保存用メモリ６１は、プロセッサチップ（図１）の内部に設けられていてもよく外部に設けられていてもよい。プログラム保存用メモリ６１は、復号装置１２の内部に設けられていてもよく外部に設けられていてもよい。暗号化されたプログラム１７は、復号装置１２に関連して設けられたプログラム保存用メモリ６１に格納されている。

【００６４】次に、図７を参照して、復号装置１２の動作を説明する。

【００６５】アドレスシャッフルを行わない場合には、アドレスシャッフル回路６２を介することなくプロセッサコア１５（または図示しないプログラムローダ）からプログラム保存用メモリ６１にアドレスがシーケンシャルに出力される。そのアドレスに従って暗号化されたプログラム１７の命令がシーケンシャルにプログラム保存用メモリ６１から読み出され、復号回路２２に供給される。復号回路２２は、復号鍵情報１８に応じて、暗号化されたプログラム１７のうちアドレスによって指定された命令を復号化する。この場合、プログラム保存用メモリ６１には暗号化されたプログラム１７の命令をシーケンシャルに予め書き込んでおく必要がある。

【００６６】アドレスシャッフルを行う場合には、プロセッサコア１５（または図示しないプログラムローダ）からシーケンシャルに出力されたアドレスがアドレスシャッフル回路６２に入力される。アドレスシャッフル回路６２は、入力されたアドレスを一定の規則に従って変換し、変換されたアドレスをプログラム保存用メモリ６１に出力する。その変換されたアドレスに従って暗号化されたプログラム１７の命令がプログラム保存用メモリ６１から読み出され、復号回路２２に供給される。復号回路２２は、復号鍵情報１８に応じて、暗号化されたプログラム１７のうちアドレスによって指定された命令を復号化する。この場合、プログラム保存用メモリ６１には暗号化されたプログラム１７の命令をアドレスシャッフル回路６２におけるアドレス変換の特性を考慮して予め書き込んでおく必要がある。

【００６７】アドレスシャッフル回路６２におけるアド

レス変換の方法としては、様々な方法が採用され得る。例えば、その方法は、偶数アドレスを奇数アドレスに変換し、奇数アドレスを偶数アドレスに変換するといった規則的にアドレスをシャッフルする方法であってもよく、まったくランダムにアドレスをシャッフルする方法であってもよい。

【００６８】なお、復号鍵情報１８を復号回路２２に直接的に入力する代わりに、図２（ａ）に示す構成と同様の構成によって復号鍵情報１８から復号鍵１８ａを得て、復号鍵１８ａを復号回路２２に入力するようにしてもよい。あるいは、復号鍵情報１８を復号鍵情報４１と復号鍵情報４２とに分割して、図４に示す構成と同様の構成によって復号鍵情報４１と復号鍵情報４２とから復号鍵１８ａを得て、復号鍵１８ａを復号回路２２に入力するようにしてもよい。あるいは、復号鍵情報１８を使用することなく、図５に示す構成と同様の構成によって選択される復号鍵を復号回路２２に入力するようにしてもよい。あるいは、復号鍵情報１８を使用することなく、図６に示す構成と同様の構成によって得られる復号鍵を復号回路２２に入力するようにしてもよい。

【００６９】なお、暗号化されたデータを格納するデータ保存用メモリを設け、アドレスシャッフル回路６２がそのデータ保存用メモリにアドレスを提供するようにしてもよい。

【００７０】（実施の形態４）以下、本発明の復号装置を含むプロセッサチップを実際のアプリケーションに適用する形態を説明する。

【００７１】図８は、電子バンキングシステム４００の構成を示す。電子バンキングシステム４００は、送信側のプロセッサチップ７１と受信側のプロセッサチップ１１とを含んでいる。プロセッサチップ７１とプロセッサチップ１１とは、通信回線４１０を介して互いに接続されている。

【００７２】プロセッサチップ７１は、暗号装置７２とインタフェース７３とプロセッサコア７５とを含む。インタフェース７３は、バス７４を介して暗号装置７２に接続されている。暗号装置７２は、暗号鍵を用いて電子バンキングデータを暗号化する暗号回路（図示せず）を含んでいる。

【００７３】プロセッサチップ１１は、復号装置１２とインタフェース１３とプロセッサコア１５とを含む。インタフェース１３は、バス１４を介して復号装置１２に接続されている。復号装置１２は、復号鍵を用いて暗号化された電子バンキングデータを復号化する復号回路（図示せず）を含んでいる。ここで、復号回路において使用される復号鍵と暗号回路において使用される暗号鍵とは同一である。復号装置１２は、実施の形態１および実施の形態２において説明した任意の構成を有し得る。

【００７４】次に、コンピュータネットワーク上で電子バンキングデータを通信する場合におけるプロセッサチップ７１およびプロセッサチップ１１の動作を説明する。

【００７５】プロセッサチップ１１は、通信回線４１０を介してプロセッサチップ７１に復号鍵情報７７を送信する。

【００７６】プロセッサチップ７１は、通信回線４１０を介して復号鍵情報７７を受信する。復号鍵情報７７は、インタフェース７３を介して暗号装置７２に入力される。また、電子バンキングデータ７８は、プロセッサチップ７１のプロセッサコア７５に入力される。プロセッサコア７５は、必要に応じて、電子バンキングデータ７８を処理する。プロセッサコア７５から出力される電子バンキングデータ７８は、暗号装置７２に供給される。暗号装置７２は、復号鍵情報７７に応じて、電子バンキングデータ７８を暗号化する。その結果、暗号化された電子バンキングデータ７６が得られる。プロセッサチップ７１は、暗号化された電子バンキングデータ７６を通信回線４１０を介してプロセッサチップ１１に送信する。

【００７７】プロセッサチップ１１は、通信回線４１０を介して暗号化された電子バンキングデータ７６を受信する。暗号化された電子バンキングデータ７６は、復号装置１２に入力される。復号装置１２は、復号鍵情報７７に応じて、暗号化された電子バンキングデータ７６を復号化する。その結果、電子バンキングデータ７８が得られる。プロセッサコア１５は、必要に応じて、電子バンキングデータ７８を処理する。プロセッサコア１５から出力される電子バンキングデータ７８は、プロセッサチップ１１の外部に出力され得る。

【００７８】このように、通信回線４１０上で通信される電子バンキングデータを暗号化することにより、電子バンキングデータ７８の秘匿性を高くすることができる。実施の形態１で述べたように復号鍵情報７７にダミーデータを挿入することにより、電子バンキングデータ７８の秘匿性をさらに高くすることができる。実施の形態２で述べたように復号装置１２の外部から入力される復号鍵情報７７と復号装置１２の内部に格納されている復号鍵情報とに基づいて、暗号化された電子バンキングデータ７６を復号化するために使用される復号鍵を生成することにより、電子バンキングデータ７８の秘匿性をさらに高くすることができる。

【００７９】なお、プロセッサチップ７１とプロセッサチップ１１との間で通信を行う際に使用される媒体は、通信回線に限定されない。そのような通信媒体は、ＩＣカードなどの磁気メディアや、光ディスクであってもよい。通信媒体として、磁気メディアや光ディスクを使用する場合には、それらに復号鍵情報を予め記憶させておく必要がある。

【００８０】さらに、暗号化されたデータの代わりに、暗号化されたプログラムをプロセッサチップ７１とプロ

セッサチップ１１との間で通信することも考えられる。例えば、そのプログラムの処理内容を受信側に知られたくない場合には、暗号化されたプログラムをプロセッサチップ７１とプロセッサチップ１１との間で通信し、かつ、復号化されたプログラムをプロセッサチップ１１の外部に出力しないように、プロセッサチップ７１とプロセッサチップ１１とを構成することが好ましい。そのようなプログラムの例としては、例えば、映像処理のプログラムが挙げられる。

【００８１】

【発明の効果】本発明の復号装置によれば、復号鍵を用いて暗号化されている情報が復号化される。その復号鍵は第１復号鍵情報と第２復号鍵情報とに基づいて生成される。第１復号鍵情報は復号装置の外部から入力され、第２復号鍵情報は復号装置の内部に格納されている。このように、復号鍵を生成するために使用される情報の一部（すなわち、第２復号鍵情報）が復号装置の内部に格納されているため、第三者が第１復号鍵情報を得た場合でも復号鍵を知ることは困難である。これにより、復号装置の外部から入力される第１復号鍵情報の機密レベルを下げることができる。その結果、第１復号鍵情報を復号装置に転送するために必要とされる回路の規模を削減することができる。

【００８２】本発明の他の復号装置によれば、復号鍵を用いて暗号化されている情報が復号化される。その復号鍵は復号鍵情報を変換することによって得られる。その復号鍵情報は、復号鍵に関連する情報と復号鍵に関連しないダミーデータとを含んでいる。復号鍵情報には復号鍵に関連しないダミーデータが含まれているため、第三者が復号鍵情報を得た場合でも復号鍵情報に含まれる復＊号鍵に関連する情報を特定することは困難である。これにより、復号鍵情報の機密レベルを下げることができる。その結果、復号鍵情報を復号装置に転送するために必要とされる回路の規模を削減することができる。

【図面の簡単な説明】

【図１】本発明の復号装置１２を含むプロセッサチップ１１の構成を示す図である。

【図２】（ａ）は復号装置１２の構成を示す図、（ｂ）および（ｃ）は復号鍵情報１８の構成例を示す図である。

【図３】抽出回路２６に入力される復号鍵情報１８のタイミングとタイミング調整回路２７から出力されるイネーブル信号のタイミングとの関係を示す図である。

【図４】復号装置１２の他の構成を示す図である。

【図５】復号装置１２の他の構成を示す図である。

【図６】復号装置１２の他の構成を示す図である。

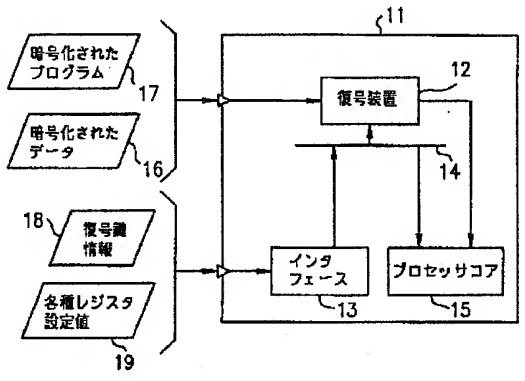
【図７】復号装置１２の他の構成を示す図である。

【図８】電子バンキングシステム４００の構成を示す図である。

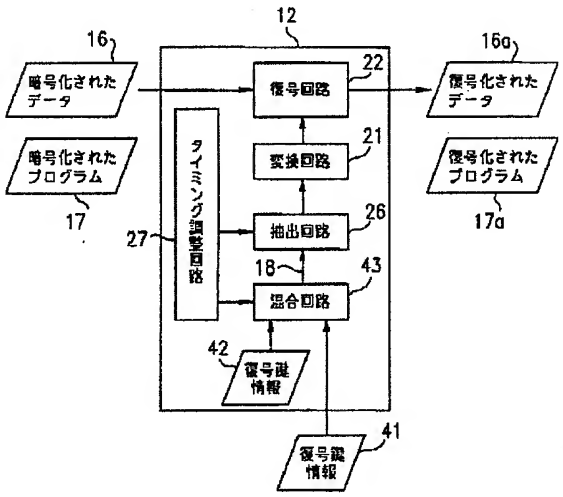
【符号の説明】

１１　プロセッサチップ
１２　復号装置
１３　インタフェース
１４　バス
１５　プロセッサコア
１６　暗号化されたデータ
１７　暗号化されたプログラム
１８　復号鍵情報
１９　各種レジスタ設定値

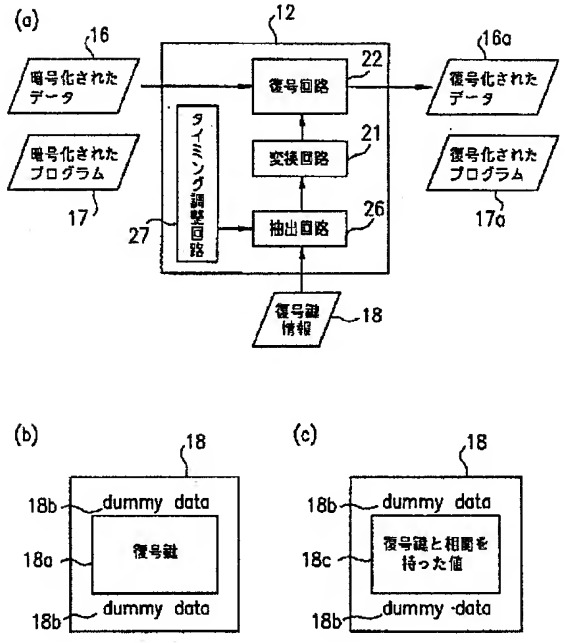
【図１】



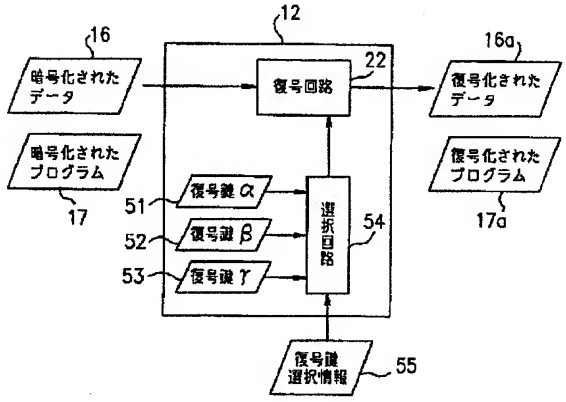
【図４】



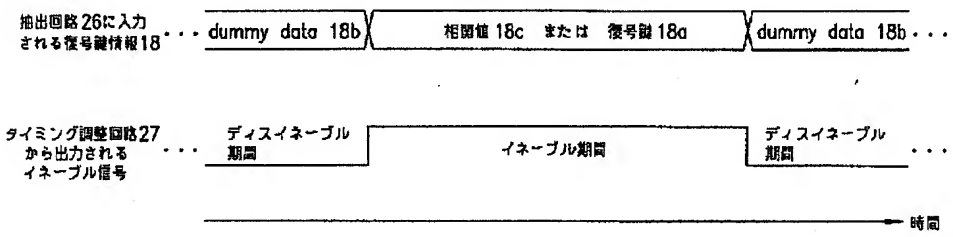
【図２】


(a)
16
暗号化されたデータ
暗号化されたプログラム
17
タイミング調整回路
27
12
復号回路
22
変換回路
21
抽出回路
26
復号鍵情報
18
16a
復号化されたデータ
復号化されたプログラム
17a
(b)
18
18b
dummy data
18a
復号鍵
dummy data
18b
(c)
18
18b
dummy data
18c
復号鍵と相関を持った値
dummy data
18b

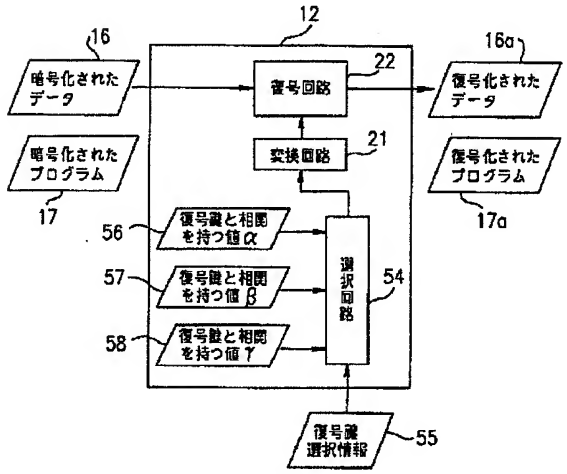
【図５】


16
暗号化されたデータ
暗号化されたプログラム
17
12
復号回路
22
復号鍵 α
51
復号鍵 β
52
復号鍵 γ
53
選択回路
54
復号鍵選択情報
55
16a
復号化されたデータ
復号化されたプログラム
17a

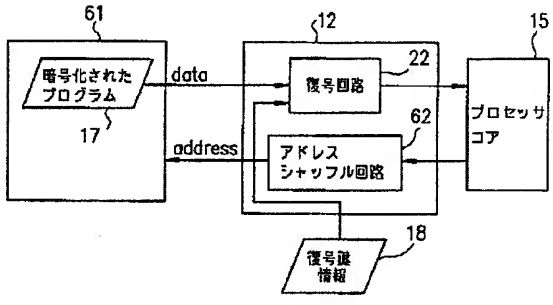
【図３】


抽出回路26に入力される復号鍵情報18
dummy data 18b
相関値 18c または 復号鍵 18a
dummy data 18b
タイミング調整回路27から出力されるイネーブル信号
ディスイネーブル期間
イネーブル期間
ディスイネーブル期間
時間

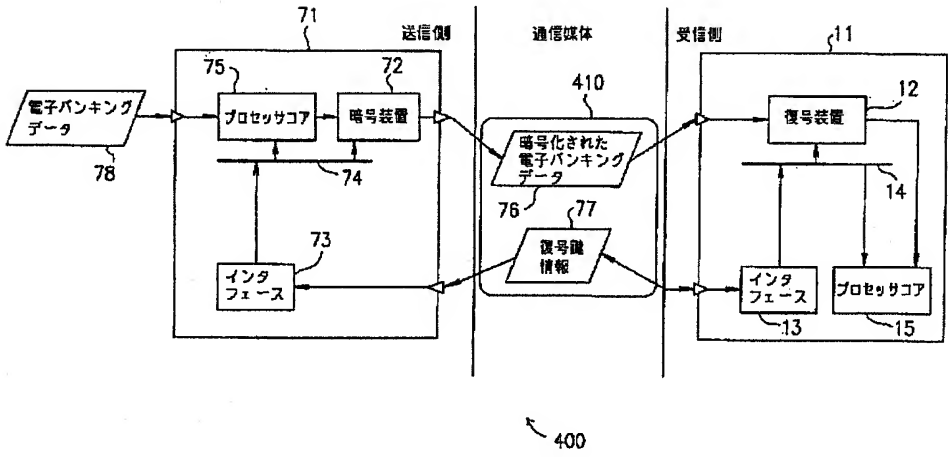
【図６】


16
暗号化されたデータ
暗号化されたプログラム
17
12
復号回路
22
変換回路
21
復号鍵と相関を持つ値 α
56
復号鍵と相関を持つ値 β
57
復号鍵と相関を持つ値 γ
58
選択回路
54
復号鍵選択情報
55
16a
復号化されたデータ
復号化されたプログラム
17a

【図７】


61
暗号化されたプログラム
17
data
address
12
復号回路
22
アドレスシャッフル回路
62
15
プロセッサコア
復号鍵情報
18

【図８】



フロントページの続き

(72)発明者　▲徳▼永　尚哉
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　寒川　賢太
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　宮口　裕
東京都港区北青山３丁目６番12号　青山富士ビル　日本テキサス・インスツルメンツ株式会社内